CHAPTER 11
SECTION 9

SYSTEM IMPLEMENTATION AND OPERATIONAL REQUIREMENTS

This section describes implementation requirements for the Duplicate Claims System. It also defines policies and procedures for the operation of the system.

1.0. SYSTEM COMPONENTS

The Duplicate Claims System is a client/server application with a run-time version of Paradox For Windows® operating as a customized graphical user interface. The application runs under Microsoft Windows For Workgroups® Version 3.11 or Microsoft Windows 95®. It resides on personal computers (PCs) and interfaces with Sybase® tables that store the Duplicate Claims Database on a Sun® server in Aurora, Colorado. Access to the Duplicate Claims System will be provided by the Government's communications network/lines (e.g., 56KB line, ISDN line, Non-classified IP Router Network). Each PC must have a color monitor, a mouse, a CD-ROM, and be configured to a printer.

2.0. HARDWARE AND SOFTWARE REQUIREMENTS

The requirements below are for user PCs, user printers, communications, software, and security.

2.1. PC Requirements

Each PC accessing the Duplicate Claims System requires the following minimum configuration:

2.1.1. Pentium 100 Megahertz (MHz) or faster IBM compatible PC

2.1.2. At least 32 Megabytes (MB) Random Access Memory (RAM)

2.1.3. One GB or larger hard drive

2.1.4. Network interface card compatible with the contractor network

2.1.5. 3.5 inch floppy disk drive

2.1.6. Super VGA (SVGA) color monitor

2.1.7. Mouse device

2.1.8. CD-ROM

2.1.9. Optionally, access to the Internet

2.2. Printer Requirements

Existing printers may be used for the Duplicate Claims System. While not required, it is strongly recommended that Hewlett Packard Series 4 or later printers with at least 4 MB RAM be used to ensure full compatibility with the reports that were designed using the Hewlett Packard LaserJet 4 Plus/4M Plus printer driver. Minor fluctuations in printer output may occur when printing reports to a non-Hewlett Packard printer.

2.3. Communications Requirements

Contractors are required to connect their PCs to the Government's communications network/lines and ensure that this connection has been tested prior to Duplicate Claims System installation. Contractors also are required to provide IP addresses for each PC to the Chief, Contractor Evaluation Branch, with a courtesy copy to the Chief, Data Systems Branch. Contractors shall immediately notify the Contractor Evaluation Branch and Data Systems Branch when IP addresses change.

2.4. Software Requirements

The software listed below must be installed and operational on each PC.

2.4.1. Operating System Software

MS-DOS 6.2 or later and Microsoft Windows For Workgroups® Version 3.11 or Windows 95 must be provided and installed by contractors.

2.4.2. Communications Software

Winsock compliant TCP/IP protocol stack must be provided and installed by contractors. The preferred choice is NetManage® TCP/IP (Chameleon, Newt), although Novell LAN Workplace LAN Workgroups, or Windows Socket TCP/IP can be used.

2.4.3. Application Software

The following applications will be provided and installed by the TMA: Paradox For Windows Runtime®, Sybase Net Library®, Duplicate Claims System application files, and Borland® SQL Links For Windows®, version 2.0.

2.4.4. Optional Software

Contractors may, at their own option and expense, procure and utilize full version database management software packages such as Microsoft® Access®, dBase®, Paradox For Windows®, etc., on the Duplicate Claims System PCs for the purpose of generating customized queries and reports utilizing the optionally downloaded tables created by the Duplicate Claims System.

2.5. Security Requirements

Security procedures require that all contractors identify a Security Manager to be responsible for overseeing the Duplicate Claims System registration process. Duplicate

Claims System registration involves the submission of four security documents which can be obtained from the TMA Home Page on the Internet. The TMA Home Page address is: http://www.tma.osd.mil. The four documents are: OCHAMPUS Form 816 (see Figure 11-9-1 on page 5); DITSO DE Form 2143 (see Figure 11-9-2 on page 6); Statement of Accountability Form (see Figure 11-9-3 on page 7); and a transmittal memorandum (see Figure 11-9-4 on page 8). Each Duplicate Claims System user must complete and sign the required forms. A single transmittal memorandum (Figure IX-4) may be used to submit the forms for a number of users.

In order to access the Duplicate Claims System, users must obtain a User ID from TMA. User IDs will be issued following receipt of properly completed registration and security forms. Users may obtain these forms from the TMA Home Page. Once on the TMA Home Page, users should go to the Systems page and click on the Duplicate Claims System button and follow the links to the required security documents. Contractor users should print a copy of each form, provide the required information, and submit the completed forms to their Duplicate Claims System Security Point of Contract for transmittal to the TMA, AIS Security Manager.

2.6. Registration and Security Forms:

2.6.1. TRICARE Duplicate Claims System Registration Form (OCHAMPUS Form 816)

Each individual user must complete and sign the top portion of the TRICARE Duplicate Claims System Registration Form (OCHAMPUS Form 816). The following are the required data elements to be provided by each user:

- Name: (Last, First, MI)
- Title:
- SSN:
- Organization: (Contractor Name, e.g., PGBA, Humana, TRIWEST, etc)
- Telephone: (include area code)
- Region/FI Contractor Numbers: (38, 45, 11, 06, 07, 13, 60, etc.)
- Complete Mailing Address:
- User's Signature

Once the user has completed this portion of the form, it should be forwarded to an individual who can provide the Site Hardware and Communications Data in the second block of the form. The following information must be provided:

- PC processor Type: (Pentium 166 Hz, etc)
- RAM: (32 MB - 40 MB, etc.)

- Hard Drive Size: (1.2 GB - 3 GB, etc.)
- CD-ROM Speed (1X, 2X, 4X, 6X, 8X, etc.)
- Operating System: (Windows 3.11, Windows 95, Windows NT)
- IP Address:
- Location of Computer: (Building Number, Unit Name, etc.)
- In-House Networking Software: (Novell Netware, Novell LAN Workplace For DOS, etc.)
- TCP/IP Protocol Stack: (NetManage Chameleon/Newt TCP/IP Version 4.5 or later, Windows TCP/IP, etc.)
- TMA Server Pinged? (The answer to this question must be "Yes" before a User ID will be issued. "Yes" verifies that the PC can establish communication with the TMA server. See Section 9, paragraph 3.0., Connectivity, for server address.)

2.6.2. Control and Prevention of Automated Information Systems (AIS) Fraud, Waste, and Abuse - DITSO-DE Form 2143, SEP 92:

Each user must sign and date this form.

2.6.3. Statement of Accountability

Each user must complete and sign the bottom section of this form. The user's supervisor/security manager must also sign and date this form.

2.6.4. Sample Memorandum (transmittal memorandum)

The three registration/security forms described above (a, b, and c) should be transmitted under a cover memorandum containing the information found on the Sample Memorandum Form. In addition to adding new Duplicate Claims System Users, the Sample Memorandum format can be used to notify TMA to delete former users of the system.

All forms must be submitted to the TMA AIS Security Manager, Data Systems Branch (ISD) for processing and assignment of User IDs and initial passwords. TMA will determine user permissions.

Upon processing of the registration and security forms, the TMA Database Administration Security POC will contact the Contractor Security Manager to inform them of new user IDs and initial passwords.

FIGURE 11-9-1 DUPLICATE SYSTEM REGISTRATION OCHAMPUS FORM 816

TRICARE DUPLICATE CLAIMS SYSTEM REGISTRATION FORM

To be completed by requester		
NAME: (Last, First, MI)	Title:	SSN: (Mandatory)
Organization:	Telephone: (incl area code):	Region / FI Contractor Numbers:*
Complete Mailing Address: (Please print)		
User's Signature:		
Site Hardware and Communications Data		
Computer Configuration:		
	IP Address:	
Location of computer:	In-House Networking Software:	
	TCP / IP Protocol Stack:	
Site Approval		
Contractor Security Manager Name:		
Contractor Security Manager Signature:		Date:
WHEN COMPLETED: TMA, AIS Security Manager (AISSM), Data System Branch		
TRICARE SUPPORT OFFICE USE ONLY		
Registration Completed: ☐ Yes ☐ No		DCS User ID:
Table Updated: ☐ Yes ☐ No	Sybase User ID:	Sybase Password:
Receipt of Documentation: ☐	Request Memorandum: ☐	Statement of Accountability: ☐
	DITSO-DE Form 2143, Sep 92: ☐	
TMA CEB Approval: ☐ Yes ☐ No	Permission Level: R / W ☐	RO ☐
FI / Contractor Number Access:		
*If access to multiple FI contracts or MCS regions is desired, all Region / FI numbers must be specified		

OCHAMPUS FORM 816
Dated 2 / 1997

FIGURE 11-9-2 DITSO DE FORM 2143

CONTROL AND PREVENTION OF AUTOMATED INFORMATION SYSTEM (AIS) FRAUD, WASTE, AND ABUSE
(This form will be used each year until filled)

I have read DISA 630-230-19 and DITSO-DE 630-230-19-R relating to the use of Automated Information Systems (AIS). I acknowledge that:

(1) All AIS resources are solely for officially designated purposes and, as such, are subject to monitoring.

(2) Any abuse of these AIS resources, including copyright violations, is prohibited.

(3) Any suspected instances of fraudulent or unauthorized uses or practices must be immediately reported to my immediate supervisor, Terminal Area Security Officer, or Information Systems Security Officer.

(4) Failure to comply may result in severe disciplinary action up to and including removal.

SIGNATURE	DATE
SIGNATURE	DATE
SIGNATURE	DATE
SIGNATURE	DATE
SIGNATURE	DATE

NOTE: If an individual refuses to sign the acknowledgment statement, the supervisor will brief the individual on the contents of this form. The supervisor must then have the refusal witnessed, and annotate this form. Failure or refusal to sign the acknowledgment statement does not excuse any violation of Department of Defense policy. The requirement to sign the acknowledgment makes sure individuals are made aware of their personal responsibilities.

DITSO-DE Form 2143, SEP 92 AFR 205-16 28 April 1989

Chapter 6
FRAUD, WASTE, AND ABUSE (FWA)

5-1. FWA Defined. AFR 123-2 formalizes the Air Force commitment to prevent and eliminate fraud, waste, and abuse. It prescribes policy, establishes procedures, and provides guidance to make sure that resources allocated to the Air Force are applied effectively to support national priorities. AFR 123-2 defines FWA as:

a. Fraud. Any intentional deception designed to unlawfully deprive the Air Force of something of value or to secure from the Air Force for an individual a benefit, privilege, allowance, or consideration to which he or she is not entitled.

b. Waste. Extravagant, careless, or needless expenditure of Air Force funds or the consumption of Air Force property that results from improper or deficient practices, systems, controls, or decisions.

c. Abuse. Intentional, wrongful, or improper use of Air Force resources.

5-2. FWA Policy. Air Force policy is that any person, military or civilian, who commits FWA on Air Force automated system resources is in direct violation of Air Force regulations and is subject to disciplinary action or prosecution by the Air Force or other appropriate agencies.

5-3. Responsibilities of Managers. Functional area managers and CFMs must get involved in the day-to-day use of automated systems. A manager must:

a. Make sure personnel use resources only for their intended purposes.

b. Establish procedures to prevent FWA in automated systems.

c. Perform periodic reviews of automated systems.

d. Establish an awareness program for users.

e. Make sure supervisors brief employees on automated system security.

f. Ensure personnel involved with automated system resource, safeguard resources and prevent FWA.

5-4. Copyright Restrictions. Do not violate copyright laws. Make sure personnel are aware of copyright restrictions placed on automated system software. Ensure users know and understand these restrictions.

FIGURE 11-9-3 STATEMENT OF ACCOUNTABILITY FORM

STATEMENT OF ACCOUNTABILITY

1. **CONFIDENTIALITY STATEMENT** - I understand and agree that, in my role as an employee, consultant, or contractor of the TRICARE Management Activity (TMA), or as an employee, consultant, or contractor of one of the Uniformed Services or Federal Agencies, I must maintain and safeguard the confidentiality of data and information acquired and/or generated by TRICARE systems which can identify and individual patient. I also understand that, in the course of my service to or relationship with, TMA, I may be privy to business-sensitive administrative, confidentiality and disclosure policies which must be followed in order that confidentiality is protected. Violation of these policies may result in immediate dismissal, may violate federal statute and may lead to criminal or civil legal action.

42 CFR 476.108 FEDERAL PENALTIES FOR UNAUTHORIZED DISCLOSURES
A person who discloses information not authorized under Title XI Part B of the Social Security Act, concerning peer review and utilization of health care, or the regulations of the part will, upon conviction, be fined no more than $1,000, or be imprisoned for no more than six months, or both, and will pay the costs of prosecution.

42 USC 290ee-3(f) and 42 USC 290dd-3(f) CRIMINAL PENALTY FOR VIOLATION
Under the statutory provisions these regulations impose restrictions upon the disclosure and use of alcohol and drug abuse patient records which are maintained in connections with the performance of any federally assisted alcohol and drug abuse program. Any person who violates any provision of these statutes shall be fined not more than $500 in the case of the first offense, and not more than $5,000 in the case of each subsequent offense.

2. **DATA SECURITY** - I understand that I may not utilize any TRICARE computer systems for non-TRICARE business purposes, and further, that I will not install any software on any of TMA's computer systems, without prior authorization from the TMA Technical Support Branch. I will not remove or transfer from the TMA premises and/or install on non-TMA computer system any TMA owned software without written permission. I will comply with all TMA procedures with respect to data confidentiality and data security.

FEDERAL PRIVACY ACT OF 1974 (5U.S.C. 552a), PUBLIC LAW 100-235 (Computer Security Act of 1987) and DODI 5200-28 apply.

SIGNATURE: _____ DATE: _____ 19_____

PRINT NAME: _____ POSITION:_____

ORGANIZATION:_____

SUPERVISOR/SECURITY
OFFICER SIGNATURE: _____ DATE: _____ 19 _____

FIGURE 11-9-4 SAMPLE MEMORANDUM

Your Agency, Department, or Business Name

TO: FRED PEREA, TMA AIS Security Manager (AISSM)
Aurora, CO 80011-9043

FROM: Your Senior Manager or Supervisor

DATE: 09/16/96

SUBJ: Issuance of User Identification for TRICARE Duplicate Claims System

Your Agency, Department, or Business Name requests that the following employees be issued a User ID for access to the TMA computer system. The following named employees require use of the TMA computer system to perform functions authorized by DoD/TMA.

As part of **Your Agency, Department, or Business Name** pre-employment processing and new employee orientation, each named employee signed a accountability/confidentiality statement. In addition, the Human Resources Function also conducted prior employer and/or reference checks. These inquiries did not reveal any derogatory or negative information regarding these employees. To reinforce their ongoing need to conduct themselves responsibly, we have had each listed employee sign additional TMA security (FWA) agreement.

The employees for whom access is requested are:

employee #1
employee #2

employee #n

Additionally, the following employees no longer require access to the TMA computer system; please remove their access:

employee #1
employee #2

employee #n

DFAS-DE Form 47(s) are attached to support the above described action(s).

Should you have any questions about this report, please contact me at **(123) 456-7890**.

Your Senior Manager or Supervisor
The Senior Manager's or Supervisor's Title
Your Agency, Department, or Business Name

3.0. CONNECTIVITY

Upon installing PCs and establishing connections to the Government's communications network/lines, contractors shall test and confirm connectivity to the TMA Sun® server. The host IP address of the Sun® server is 159.133.84.3.

4.0. PC PLACEMENT

Contractors shall determine the best placement of the PCs operating the Duplicate Claims System. One possible four-PC placement configuration might be as follows:

4.1. One PC in the work unit where potential duplicate claims are researched and determinations made that actual duplicate payments were made.

4.2. One PC in the work unit responsible for initiating recoupments.

4.3. One PC in the work unit where refunds and offsets are collected.

4.4. One PC in the work unit where claims adjustments are made.

User PCs may be configured to access contractor proprietary claims processing systems or placed next to contractor proprietary system terminals. One advantage of configuring the Duplicate Claims System PCs to also access contractor proprietary system files is that only one computer would be needed at a particular workstation. One disadvantage is that a user would have to constantly switch back and forth from the Duplicate Claims System to the claims processing system screens to perform various research and resolution functions. Contractors should assess the best placement of PCs based on their own work needs and styles of working, and subsequently locate PCs where duplicate claims resolution functions will be performed most efficiently.

5.0. SYSTEM SUPPORT

For Duplicate Claims System support, contractors should call the **TMA Help Desk at 1-303-676-3800**. System upgrades will occur automatically when users sign on to the system.

6.0. SYSTEM INSTALLATION AND TRAINING

6.1. Contractor Installation Responsibilities

Contractors are responsible for installing PCs, connecting them to the network, and ensuring that connectivity is established to the TMA SUN® server. In addition to the communications software required to establish connectivity to the TMA server, contractors are responsible for installing Windows®.

6.2. TMA Installation Responsibilities

The TMA will provide and install Paradox For Windows Runtime®, the Duplicate Claims System application files, Sybase Net Library®, and Borland® SQL Links For Windows® Version 2.0. To facilitate the TMA installation process, each contractor shall make available at least one data systems support staff to assist during the installation process and to serve as a liaison between TMA installation personnel and contractor data systems personnel.

6.3. Training

TMA will provide hands-on training to prospective users of the Duplicate Claims System at designated contractor sites. Up to two days of training per regional contract may be provided prior to system implementation and full-scale operation. The TMA will coordinate training schedules with each contractor. Efforts will be made during the coordination process to consolidate the training of staff for contractors with responsibility for more than one regional contract. For example, if a contractor has responsibility for two regional contracts and the duplicate claims resolution activities for both contracts will occur at the same geographical site, efforts will be made to consolidate the training of staff for both regions into one training session instead of two.

Each contractor shall provide a training room at each training site. The training room shall be equipped with a sufficient number of chairs and tables to accommodate the number of staff to be trained. A chalkboard or whiteboard and an overhead projector also should be provided. At least one of the Duplicate Claims System PCs should be temporarily installed in the training room for training purposes. The TMA will use traditional lecture-type training, and hands-on exercises to ensure that users are comfortable with the system at the conclusion of each training session.

7.0. CONTRACTOR POINTS OF CONTACT

To resolve multi-contractor duplicate claim sets, contractors are required to communicate and coordinate with each other (see Section 6, Resolving Multi-Contractor Claim Sets). For each regional contract for which a contractor is responsible, the contractor is required to identify at least one individual to serve as the Duplicate Claims System point of contact (POC). Contractor POCs must be individuals who are, or will be, trained in the use of the Duplicate Claims System, and are able to perform the required research and determine whether a particular claim is within their processing jurisdiction. For each regional contract for which they are responsible, contractors shall provide the name(s), title(s), business address(es) and business telephone number(s) of their point(s) of contact to the Contracting Officer, with courtesy copies to the Chief, Contractor Evaluation Branch, Chief, Managed Care Support Branch A and the Chief, Managed Care Support Branch B. The POCs shall be provided to the Contracting Officer no later than two weeks prior to implementation of the Duplicate Claims System.

Prior to system implementation, the TMA Contractor Evaluation Branch will provide each contractor with the list of all Duplicate Claims System POCs. Whenever a new contract is awarded, the TMA Contractor Evaluation Branch will notify all contractors of the new Contractor's POC. Once the initial listing is provided to the contractors, it is the responsibility of each contractor to maintain the listing and keep TMA and the other contractors informed of any changes.

Contractors shall notify the Contracting Officer, the Contractor Evaluation Branch, the Managed Care Support Branch A, the Managed Care Support Branch B and the other contractor POCs in writing within five working days of any POC change. Also, by September 1 of each year, contractors are required to provide the Contracting Officer with the list of names, titles, business addresses and business telephone numbers of their POCs. Courtesy copies of the listings shall be provided to the Contractor Evaluation Branch, Managed Care / Support Branch A, / Managed Care Support Branch B, and all contractor POCs.

8.0. OPERATING PROCEDURES

For each regional contract for which a contractor is responsible, the contractor shall develop internal operating procedures for the Duplicate Claims System. These internal operating procedures shall designate the responsible areas for the various duplicate claims resolution functions and establish time lines. For example, one contractor may decide that the adjustment unit shall be responsible for scanning the Duplicate Claims System on a weekly basis for the appearance of adjustments submitted and for closing sets. Another contractor may decide that the unit responsible for researching potential duplicate claims should also be responsible for scanning for adjustments and closing the sets on a daily basis.

Contractor contract requirements for overpayment recovery, refunds and offsets, adjustments, etc., including timeliness requirements, apply to the operation of the Duplicate Claims System. As a result, operating procedures must be developed which are consistent with all applicable contract requirements. Procedures must be established to ensure that recoupments are initiated in a timely manner following the research determination that a duplicate payment had been made. In other words, procedures must specify that after a decision has been made by the person responsible for determining that a duplicate payment was made, recoupment must be initiated in a timely manner and must be consistent with all overpayment recovery timeliness standards.

Contractors shall develop these procedures within 45 days of the date of system implementation and submit them to the Contracting Officer for review and approval.

9.0. TRANSITIONS

The date when an incoming contractor will assume full responsibility for resolving all existing potential duplicate claim sets from the outgoing contractor (including completing existing recoupments), and for all new potential duplicate claim sets, shall be determined during transition meetings and be established in the transition plan/schedule. The criteria for the types of claims for which the outgoing contractor will retain responsibility (e.g., network/non-network), and the types of claims to be transferred to the incoming contractor, will also be defined in the transition plan/schedule. The contractor Evaluation Branch shall be informed by MCA and MCB of the type of claims to be transferred to the incoming contractor and the date upon which Duplicate Claim Sets containing these types of claims should be transferred to the incoming contractor.